

340000540 US1

16869P018200

#2

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 3月30日

出 願 番 号

Application Number:

特願2000-094313

出 願 人

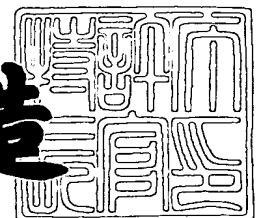
Applicant (s):

株式会社日立製作所

2000年10月 6日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3081671

【書類名】 特許願

【整理番号】 K00005401

【提出日】 平成12年 3月30日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/00

【発明者】

 【住所又は居所】 東京都江東区新砂一丁目6番27号 株式会社日立製作所 公共システム事業部内

 【氏名】 篠田 隆志

【発明者】

 【住所又は居所】 東京都江東区新砂一丁目6番27号 株式会社日立製作所 公共システム事業部内

 【氏名】 豊島 久

【発明者】

 【住所又は居所】 東京都江東区新砂一丁目6番27号 株式会社日立製作所 公共システム事業部内

 【氏名】 中島 純三

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社日立製作所

【代理人】

 【識別番号】 100083552

 【弁理士】

 【氏名又は名称】 秋田 収喜

 【電話番号】 03-3893-6221

【手数料の表示】

 【予納台帳番号】 014579

 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ改竄検知方法及びその実施装置並びにその処理プログラムを記録した記録媒体

【特許請求の範囲】

【請求項 1】 コンテンツの改竄を検知するコンテンツ改竄検知方法において、

複数のコンテンツの現在の構成または内容に対応する改竄検知情報を生成するステップと、当該コンテンツの登録または更新時の構成または内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知するステップとを有することを特徴とするコンテンツ改竄検知方法。

【請求項 2】 コンテンツの改竄を検知するコンテンツ改竄検知方法において、

あるコンテンツについて、その改竄を検知する為の改竄検知情報が生成済みであるかどうかを検査するステップと、当該コンテンツの改竄検知情報の有無を検査するステップとを有することを特徴とするコンテンツ改竄検知方法。

【請求項 3】 コンテンツの改竄を検知するコンテンツ改竄検知方法において、

コンテンツの現在の内容に対応する改竄検知情報を生成するステップと、当該コンテンツの登録または更新時の内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知した場合に、当該コンテンツの要求元、登録元または更新元に通知するステップとを有することを特徴とするコンテンツ改竄検知方法。

【請求項 4】 コンテンツの改竄を検知するコンテンツ改竄検知装置において、

複数のコンテンツの現在の構成または内容に対応する改竄検知情報を生成する改竄検知情報生成処理部と、当該コンテンツの登録または更新時の構成または内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知する改竄検知処理部とを備えることを特徴とするコンテンツ改竄検知装置。

【請求項 5】 コンテンツの改竄を検知するコンテンツ改竄検知装置としてコンピュータを機能させる為のプログラムを記録したコンピュータ読み取り可能な記録媒体において、

複数のコンテンツの現在の構成または内容に対応する改竄検知情報を生成する改竄検知情報生成処理部と、当該コンテンツの登録または更新時の構成または内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知する改竄検知処理部としてコンピュータを機能させる為のプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明はコンテンツの改竄を検知するコンテンツ改竄検知装置に関し、特にインターネットのホームページで表示されるコンテンツに対して行われた改竄を検知するコンテンツ改竄検知装置に適用して有効な技術に関するものである。

【 0 0 0 2 】

【従来の技術】

従来、個人を始め官公庁や多くの企業等がWWW(World Wide Web)サーバ装置にホームページを開設し、各種の情報発信を行っている。官公庁や企業が開設するホームページで公開される内容は、簡単なお知らせから公式な発表と同等な内容のものまで多岐に渡っており、インターネットにアクセスすることにより誰でもこれらの情報を得ることができる様になっている。

【 0 0 0 3 】

これらの官公庁や企業が開設するホームページの内容は、その官公庁や企業が外部に対して正式に発信しているものと考えられる為、その内容に誤りがあったり、外部の人間によるサーバへの不正侵入によりホームページの内容が改竄された場合、著しい信用の低下を招く場合がある。この為、簡単な広報活動の為にホームページを開設している場合であっても、そのセキュリティ対策を十分にとっておく必要があるが、近年では外部の人間が官公庁等のサーバに不正侵入し、ホームページの内容を改竄するという事件が相次いでいる。

【 0 0 0 4 】

なお厳密な電子データの真正性の認証を可能とすると共に、その真正性を視覚的に電子データの利用者に表現する認証可能な電子データの生成方法については、特開 2 0 0 0 - 7 8 1 2 5 号公報に記載されている。その概要は、Web ページや商標などの電子マーク B を認証するための認証情報にデジタル署名を付加したものを、電子マーク A に不可視の電子透かしとして埋め込んだ後、真正性を視覚的に表現する電子マーク A を、電子マーク B に可視の電子透かしとして埋め込むものである。

【 0 0 0 5 】

【発明が解決しようとする課題】

前記の様なホームページの内容を改竄される事件での大きな問題は、ホームページを公開するサーバのセキュリティ対策が甘いということに加え、公開しているホームページの量が膨大である為、一部のホームページが改竄されてもそれに気付くのが遅れがちになるという点にある。

【 0 0 0 6 】

本発明の目的は上記問題を解決し、コンテンツの改竄を早期発見することが可能な技術を提供することにある。

【 0 0 0 7 】

本発明の他の目的は改竄検知情報の除去による改竄の隠蔽を防止することが可能な技術を提供することにある。

【 0 0 0 8 】

本発明の他の目的は改竄が行われた位置を特定することが可能な技術を提供することにある。

【 0 0 0 9 】

【課題を解決するための手段】

本発明は、コンテンツの改竄を検知するコンテンツ改竄検知装置において、複数のコンテンツの構成または内容の改竄を検知するものである。

【 0 0 1 0 】

本発明では、複数のコンテンツの登録または更新時にそれらの構成または内容

に対応する改竄検知情報を生成しておく。そして、所定の時刻になる等の所定の条件が成立した場合に、前記生成した改竄検知情報を参照し、当該コンテンツの現在の構成または内容に対応する改竄検知情報を生成した後、前記参照した改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知し、当該コンテンツの改竄を通知する。

【 0 0 1 1 】

例えば、公開しているホームページで表示される複数のコンテンツの登録または更新時に、それらのファイル構造や各ファイルの内容のハッシュ値を改竄検知情報として生成して I M (Internet-Marks) に埋め込み、ホームページのトップページにその I M を貼付しておく。

【 0 0 1 2 】

そして、常駐プログラム等の処理により所定の時刻になる等の所定の条件が成立した場合に、前記貼付した I M 中の登録または更新時のファイル構造や各ファイルの内容のハッシュ値を参照し、また現在のファイル構成や各ファイルの内容のハッシュ計算を行う。次に、前記参照した I M 中の登録または更新時のファイル構造や各ファイルの内容のハッシュ値と、前記生成した現在のファイル構成や各ファイルの内容のハッシュ値とを比較し、もし前記生成した現在のハッシュ値が I M に埋め込まれているハッシュ値と異なる場合は、システム管理者に通報すると共に、トップページの I M のデザインを変更してコンテンツの改竄が行われたことを閲覧者に知らせる。

【 0 0 1 3 】

前記の様に本発明では、システム管理者等の人間が常時チェックしなくても、公開しているホームページの一部が改竄された場合に、改竄が行われたことを即座に通知することが可能となり、不正の早期発見ができる。また同時に、閲覧者に対してもホームページの改竄が行われたことを即座に知らせることが可能となる。

【 0 0 1 4 】

以上の様に本発明のコンテンツ改竄検知装置によれば、複数のコンテンツの構成または内容の改竄を検知するので、コンテンツの改竄を早期発見することが可

能である。

【0015】

【発明の実施の形態】

(実施形態1)

以下に複数のコンテンツの改竄を検知する実施形態1のコンテンツ改竄検知装置について説明する。

【0016】

図1は本実施形態のコンテンツ改竄検知装置の概略構成を示す図である。図1に示す様に本実施形態のサーバ装置100は、CPU101と、メモリ102と、磁気ディスク装置103と、入力装置104と、出力装置105と、CD-ROM装置106と、コンテンツデータ107と、IM108とを有している。

【0017】

CPU101は、サーバ装置100全体の動作を制御する装置である。メモリ102は、サーバ装置100全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置103は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【0018】

入力装置104は、複数のコンテンツの改竄を検知する為の各種入力を行う装置である。出力装置105は、複数のコンテンツの改竄の検知に伴う各種出力を行う装置である。CD-ROM装置106は、前記各種処理プログラムを記録したCD-ROMの内容を読み出す装置である。

【0019】

コンテンツデータ107は、クライアント装置120からの要求に応じて公開されるページの内容を示すデータである。IM108は、複数のコンテンツデータ107に対応する改竄検知情報を埋め込んだ画像データである。

【0020】

またサーバ装置100は、IM生成処理部110と、改竄検知情報生成処理部111と、改竄検知処理部112とを有している。

【0021】

IM生成処理部110は、複数のコンテンツの登録または更新時の構成または内容に対応する改竄検知情報を埋め込んだIMを生成する処理部である。改竄検知情報生成処理部111は、複数のコンテンツの構成または内容に対応する改竄検知情報を生成する処理部である。

【0022】

改竄検知処理部112は、複数のコンテンツの登録または更新時の構成または内容に対応する改竄検知情報と、当該コンテンツの現在の構成または内容に対応する改竄検知情報とを比較して当該コンテンツの改竄を検知する処理部である。

【0023】

サーバ装置100をIM生成処理部110、改竄検知情報生成処理部111及び改竄検知処理部112として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。

【0024】

コンテンツデータを管理・公開するサーバ装置100と、コンテンツデータを閲覧するクライアント装置120は、インターネット等のネットワークにより相互にデータの送受信が可能であるものとする。

【0025】

サーバ装置100には、クライアント装置120からの要求に応じてコンテンツデータの公開を行うWWWサーバが実装され、クライアント装置120には、サーバ装置からコンテンツデータを受信し、表示するWWWブラウザが実装される。

【0026】

また、サーバ装置100に接続される磁気ディスク装置103には、複数のコンテンツデータ107を格納し、そのうちの1つ、例えばコンテンツのトップページに、複数のコンテンツデータ107に対応する改竄検知情報を埋め込んだインターネットマークであるIM108を貼付することとする。

【0027】

図 2 は本実施形態の IM 生成処理部 1 1 0 の処理手順を示すフローチャートである。図 2 に示す様にサーバ装置 1 0 0 の IM 生成処理部 1 1 0 は、複数のコンテンツの登録または更新時の構成または内容に対応する改竄検知情報を埋め込んだ IM を生成する処理を行う。

【 0 0 2 8 】

ステップ 2 0 1 で IM 生成処理部 1 1 0 は、複数のコンテンツの構成に対応する改竄検知情報として、複数のコンテンツを構成する各コンテンツのパス名（ディレクトリ名）を含むファイル名に対応したハッシュ値を改竄検知情報生成処理部 1 1 1 により生成し、ステップ 2 0 2 では、ステップ 2 0 1 で生成した改竄検知情報を IM 1 0 8 に埋め込む。

【 0 0 2 9 】

ステップ 2 0 3 で IM 生成処理部 1 1 0 は、複数のコンテンツの内容に対応する改竄検知情報として、複数のコンテンツを構成する各コンテンツデータ 1 0 7 の内容に対応したハッシュ値を改竄検知情報生成処理部 1 1 1 により生成する。ステップ 2 0 4 では、ステップ 2 0 3 で生成した改竄検知情報を IM 1 0 8 に埋め込み、前記の様に複数のコンテンツの改竄検知情報が埋め込まれた IM 1 0 8 をトップページに貼付ける。

【 0 0 3 0 】

図 3 は本実施形態のパス名を含むファイル名に対応したハッシュ値の生成処理の概要を示す図である。図 3 に示す様にステップ 2 0 1 の処理では、改竄検知情報生成の対象となるコンテンツデータ 1 0 7 のパス名付きのファイル名 3 0 0 を取得し、取得したファイル名 3 0 0 の並びが一意に決定する様、取得したファイル名 3 0 0 をアルファベット順等でソートした後、それらのファイル名 3 0 0 のデータを連結してハッシュ値 3 2 0 を計算する。

【 0 0 3 1 】

図 4 は本実施形態のパス名を含むファイル名に対応したハッシュ値の生成処理の処理手順を示すフローチャートである。図 4 に示す様にサーバ装置 1 0 0 の改竄検知情報生成処理部 1 1 1 は、複数のコンテンツのパス名を含むファイル名に対応する改竄検知情報を生成する処理を行う。

【0032】

ステップ401で改竄検知情報生成処理部111は、改竄検知情報の生成の対象となるコンテンツを選択し、そのコンテンツデータ107のパス名付きのファイル名300を取得する。例えばサーバ装置100で公開しているホームページのトップページ以下に存在しているHTML(Hyper Text Markup Language)やXML(eXtensible Markup Language)等のWebページを記述する為の記述言語で記載されたファイルやそれらのファイルにより表示される画像ファイルを選択したり、またトップページからリンクしているページの中でサーバ装置100内に存在しているページのファイルそれらのファイルにより表示される画像ファイルを選択する。また改竄検知情報を生成するファイルを定義した生成情報を別途作成し、この生成情報に従ってサーバ装置100中の特定のファイルについてのみ改竄検知情報を生成するものとしても良い。

【0033】

ステップ402では、ステップ401で取得したファイル名300の並びが一意に決定する様、取得したファイル名300をアルファベット順等でソートする。そしてステップ403では、それらのファイル名300のデータを連結し、ステップ404では、前記連結したファイル名300のデータについてのハッシュ値320を計算する。

【0034】

図5は本実施形態のコンテンツの内容に対応したハッシュ値の生成処理の概要を示す図である。図5に示す様にステップ203の処理では、先程取得したファイル名310のそれぞれについて、対応する実際のコンテンツデータ500を取得する。更に、各コンテンツデータのハッシュ値510を計算する。次に、それらのハッシュ値510を連結し、それについてのハッシュ値520を計算する。

【0035】

図6は本実施形態のコンテンツの内容に対応したハッシュ値の生成処理の処理手順を示すフローチャートである。図6に示す様にサーバ装置100の改竄検知情報生成処理部111は、複数のコンテンツのコンテンツデータに対応する改竄検知情報を生成する処理を行う。

【0036】

ステップ601で改竄検知情報生成処理部111は、先程取得したファイル名310のそれぞれについて、対応する実際のコンテンツデータ500を取得し、ステップ602では、各コンテンツデータ500のハッシュ値510を計算する。

【0037】

ステップ603では、各コンテンツデータ500のハッシュ値510を連結し、ステップ604では、前記連結したハッシュ値510についてのハッシュ値520を計算する。

【0038】

前記の様にIM108に埋め込むファイル名300のハッシュ値320及びコンテンツデータ500のハッシュ値520は、コンテンツの改竄を検知する時に、正しい値として使用するものである。従って、コンテンツデータ500の内容やファイル構成を変更した場合は、その都度、上記の通り各々のハッシュ値を計算し、IM108に埋め込み直す必要がある。但し、コンテンツデータ500が変更される都度、IM108を自動生成し、コンテンツデータ500に自動貼付するようなジェネレータを用意することで、利用者の操作を不要とすることも可能である。

【0039】

図7は本実施形態の改竄検知処理部112の処理手順を示すフローチャートである。図7に示す様にサーバ装置100の改竄検知処理部112は、複数のコンテンツの登録または更新時の構成または内容に対応する改竄検知情報と、当該コンテンツの現在の構成または内容に対応する改竄検知情報とを比較して当該コンテンツの改竄を検知する処理を行う。

【0040】

ステップ701で改竄検知処理部112は、図4に示した処理と同様にして複数のコンテンツを構成する各コンテンツについてそれらのパス名を含むファイル名に対するハッシュ値を改竄検知情報生成処理部111により計算する。

【0041】

ステップ702では、IM108内に埋め込まれているハッシュ値320と前記計算したハッシュ値の値とを比較し、IM108内に埋め込まれているハッシュ値320が前記計算したハッシュ値と異なる場合にはステップ703へ進む。

【0042】

前記パス名を含むファイル名に対するハッシュ値の相違は、コンテンツデータ107のファイル構成の改竄(コンテンツデータ107の削除・追加等)が行われたことを表している。従ってステップ703では、ファイル構成の改竄が行われたことを示す改竄通告を行う。改竄通告の方法としては、例えばシステム管理者のコンソール画面にメッセージを表示したり、或いは閲覧者がコンテンツのトップページを参照した時、IM108の画像デザインを変更し、コンテンツの改竄がなされていることを示す等が考えられる。

【0043】

ステップ704では、図6で示した処理と同様にして複数のコンテンツを構成する各コンテンツについてそれらの各コンテンツデータ500に対するハッシュ値を改竄検知情報生成処理部111により計算する。

【0044】

ステップ705では、IM108内に埋め込まれているハッシュ値520と前記計算したハッシュ値の値とを比較し、IM108内に埋め込まれているハッシュ値520が前記計算したハッシュ値と異なる場合にはステップ706へ進む。

【0045】

前記各コンテンツデータ500に対するハッシュ値の相違は、コンテンツデータ500のファイル内容の改竄(コンテンツの文章の一部変更等)が行われたことを表している。従って、ステップ706では、ファイル内容の改竄が行われたことを示す改竄通告を行う。

【0046】

本実施形態では、改竄を検知する為の元データとして、パス付きのファイル名及び実際のコンテンツデータを用いているが、これらに加え、ファイル属性、コンテンツに貼付されている各種データ、リンクされている他のコンテンツ等を含めても良い。また、改竄を検知する為の情報として、ディレクトリやファイルの

更新日時等を用いても良い。

【 0 0 4 7 】

本実施形態では、改竄検知情報としてハッシュ値を計算し、IMに埋め込んでいるが、これはデータの容量を少なく抑えることが目的である。従ってハッシュ値を計算せず、パス付きファイル名のデータや各コンテンツデータをそのままIMに埋め込んでも良い。また、各コンテンツデータ500のハッシュ値510をそのままIMに埋め込んだり、各コンテンツデータ500を連結し、それに対して計算したハッシュ値をIMに埋め込む形態も可能である（コンテンツデータを特定する情報が残る形態であれば良い）。

【 0 0 4 8 】

本実施形態では、改竄検知情報をトップページのIMに格納したが、各コンテンツ毎にIMを貼付しても良い。また、改竄検知情報をIMに埋め込むのではなく、デジタル署名としたり或いは加工せずにそのままの状態で磁気ディスク装置103内に格納しても良い。

【 0 0 4 9 】

本実施形態において改竄検知処理部112を起動させる際には、サーバ装置100の管理者等の手により手動で起動させる以外に、定期的に自動起動させたり、メモリに常駐させて常時検知を行ったり、また、閲覧者がコンテンツデータを参照した時に自動起動させる等の処理を行っても良い。

【 0 0 5 0 】

以上説明した様に本実施形態のコンテンツ改竄検知装置によれば、複数のコンテンツの構成または内容の改竄を検知するので、コンテンツの改竄を早期発見することが可能である。

（実施形態2）

以下にEXITゲートを用いて改竄検知情報の有無を検知すると共に改竄位置を特定する実施形態2のコンテンツ改竄検知装置について説明する。

【 0 0 5 1 】

図8は本実施形態のコンテンツ改竄検知装置の概要を示す図である。図8に示す様に本実施形態の改竄検知システムは、サーバ装置800と、EXITゲート

装置 8 1 0 と、クライアント装置 8 2 0 とを有している。

【 0 0 5 2 】

サーバ装置 8 0 0 は、コンテンツの登録または更新時の内容に対応する改竄検知情報を埋め込んだ IM を貼付してコンテンツを生成し、EXIT ゲート装置 8 1 0 を介してクライアント装置 8 2 0 へ当該コンテンツを送信する装置である。

【 0 0 5 3 】

EXIT ゲート装置 8 1 0 は、クライアント装置 8 2 0 から要求されたコンテンツの改竄を検知する装置である。クライアント装置 8 2 0 は、EXIT ゲート装置 8 1 0 から受け取ったコンテンツの改竄を検知し、改竄の行われていないコンテンツを表示する装置である。

【 0 0 5 4 】

図 8 に示す様に本実施形態では、サーバ装置 8 0 0 とクライアント装置 8 2 0 との間に EXIT ゲート装置 8 1 0 を設け、EXIT ゲート装置 8 1 0 にて IM の有無のチェックや IM を用いた改竄検知を行う。またクライアント装置 8 2 0 でのチェックを併用することにより、サーバ装置 8 0 0 上またはサーバ装置 8 0 0 から EXIT ゲート装置 8 1 0 までの経路上、若しくは EXIT ゲート装置 8 1 0 からクライアント装置 8 2 0 までの経路上で改竄が行われているかどうかをチェックする。

【 0 0 5 5 】

図 9 は本実施形態のサーバ装置 8 0 0 の概略構成を示す図である。図 9 に示す様に本実施形態のサーバ装置 8 0 0 は、CPU 9 0 1 と、メモリ 9 0 2 と、磁気ディスク装置 9 0 3 と、入力装置 9 0 4 と、出力装置 9 0 5 と、CD-ROM 装置 9 0 6 と、コンテンツデータ 9 0 7 と、IM 9 0 8 と、生成情報 9 0 9 とを有している。

【 0 0 5 6 】

CPU 9 0 1 は、サーバ装置 8 0 0 全体の動作を制御する装置である。メモリ 9 0 2 は、サーバ装置 8 0 0 全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置 9 0 3 は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【 0 0 5 7 】

入力装置 9 0 4 は、コンテンツを登録したり更新する為の各種入力を行う装置である。出力装置 9 0 5 は、コンテンツの登録や更新に伴う各種出力を行う装置である。CD-ROM 装置 9 0 6 は、前記各種処理プログラムを記録した CD-ROM の内容を読み出す装置である。

【 0 0 5 8 】

コンテンツデータ 9 0 7 は、クライアント装置 1 2 0 からの要求に応じて公開されるページの内容を示すデータである。IM 9 0 8 は、コンテンツデータ 9 0 7 に対応する改竄検知情報を埋め込んだ画像データである。生成情報 9 0 9 は、コンテンツの改竄を検知する為の改竄検知情報が生成されたコンテンツを示すデータである。

【 0 0 5 9 】

またサーバ装置 8 0 0 は、IM 生成処理部 9 1 0 と、改竄検知情報生成処理部 9 1 1 と、生成情報作成処理部 9 1 2 と、改竄通知受信処理部 9 1 3 とを有している。

【 0 0 6 0 】

IM 生成処理部 9 1 0 は、コンテンツの内容に対応する改竄検知情報を埋め込んだ IM 9 0 8 を生成する処理部である。改竄検知情報生成処理部 9 1 1 は、コンテンツの内容に対応する改竄検知情報を生成する処理部である。

【 0 0 6 1 】

生成情報作成処理部 9 1 2 は、コンテンツの改竄を検知する為の改竄検知情報が生成されたコンテンツを示す生成情報 9 0 9 を作成する処理部である。改竄通知受信処理部 9 1 3 は、コンテンツの改竄が行われていることを示す通知を EX IT ゲート装置 8 1 0 から受信する処理部である。

【 0 0 6 2 】

サーバ装置 8 0 0 を IM 生成処理部 9 1 0、改竄検知情報生成処理部 9 1 1、生成情報作成処理部 9 1 2 及び改竄通知受信処理部 9 1 3 として機能させる為のプログラムは、CD-ROM 等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録

する記録媒体はCD-ROM以外の他の記録媒体でも良い。

【0063】

図10は本実施形態のEXITゲート装置810の概略構成を示す図である。図10に示す様に本実施形態のEXITゲート装置810は、CPU1001と、メモリ1002と、磁気ディスク装置1003と、入力装置1004と、出力装置1005と、CD-ROM装置1006とを有している。

【0064】

CPU1001は、EXITゲート装置810全体の動作を制御する装置である。メモリ1002は、EXITゲート装置810全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【0065】

磁気ディスク装置1003は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置1004は、コンテンツの改竄を検知する為の各種入力を行う装置である。出力装置1005は、コンテンツの改竄の検知に伴う各種出力を行う装置である。CD-ROM装置1006は、前記各種処理プログラムを記録したCD-ROMの内容を読み出す装置である。

【0066】

またEXITゲート装置810は、生成検査処理部1010と、存在検査処理部1011と、改竄検知情報生成処理部1012と、改竄検知処理部1013とを有している。

【0067】

生成検査処理部1010は、コンテンツの改竄を検知する為の改竄検知情報が生成されたコンテンツを示す生成情報909を参照し、クライアント装置820から要求されたコンテンツについて、その改竄を検知する為の改竄検知情報が生成済みであるかどうかを検査する処理部である。

【0068】

存在検査処理部1011は、クライアント装置820から要求されたコンテンツについて、そのコンテンツの改竄検知情報の有無を検査する処理部である。改竄検知情報生成処理部1012は、クライアント装置820から要求されたコン

テンツの現在の内容に対応する改竄検知情報を生成する処理部である。

【0069】

改竄検知処理部1013は、当該コンテンツの登録または更新時の内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知した場合に、サーバ装置800上またはサーバ装置800からEXITゲート装置810までの経路上での当該コンテンツの改竄を検知したことを当該コンテンツの要求元であるクライアント装置820、登録元及び更新元であるサーバ装置800に通知する処理部である。

【0070】

EXITゲート装置810を生成検査処理部1010、存在検査処理部1011、改竄検知情報生成処理部1012及び改竄検知処理部1013として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。

【0071】

図11は本実施形態のクライアント装置820の概略構成を示す図である。図11に示す様に本実施形態のクライアント装置820は、CPU1101と、メモリ1102と、磁気ディスク装置1103と、入力装置1104と、出力装置1105と、CD-ROM装置1106とを有している。

【0072】

CPU1101は、クライアント装置820全体の動作を制御する装置である。メモリ1102は、クライアント装置820全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【0073】

磁気ディスク装置1103は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置1104は、コンテンツを要求して表示する為の各種入力を行う装置である。出力装置1105は、コンテンツの要求に伴ってコンテンツを表示する装置である。CD-ROM装置1106は、前記各種処理プログラムを記録したCD-ROMの内容を読み出す装置である。

【0074】

またクライアント装置820は、改竄検知情報生成処理部1110と、改竄検知処理部1111とを有している。

【0075】

改竄検知情報生成処理部1110は、要求したコンテンツをEXITゲート装置810から受け取り、そのコンテンツの現在の内容に対応する改竄検知情報を生成する処理部である。改竄検知処理部1111は、当該コンテンツの登録または更新時の内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知した場合に、EXITゲート装置810からクライアント装置820までの経路上での当該コンテンツの改竄を検知したことを示す表示を行う処理部である。

【0076】

クライアント装置820を改竄検知情報生成処理部1110及び改竄検知処理部1111として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。

【0077】

図12は本実施形態のコンテンツ登録／更新処理の処理手順を示すフローチャートである。図12に示す様にサーバ装置800では、登録や更新が行われたコンテンツの内容に対応する改竄検知情報を埋め込んだIM908を生成して当該コンテンツに貼付けた後、IM908の貼付けが行われたコンテンツを示す生成情報909を作成する処理を行う。

【0078】

ステップ1201でIM生成処理部910は、コンテンツデータ907の登録や更新が行われたかどうかを調べ、コンテンツデータ907の登録や更新が行われている場合にはステップ1202へ進む。

【0079】

ステップ1202では、登録や更新が行われたコンテンツについて、そのコン

テンツデータ 9 0 7 のハッシュ値を改竄検知情報生成処理部 9 1 1 により計算し、その内容に対応する改竄検知情報として IM 9 0 8 に埋め込む。そしてステップ 1 2 0 3 では、ステップ 1 2 0 2 で改竄検知情報を埋め込んだ IM 9 0 8 を、前記登録や更新が行われたコンテンツに貼付ける。

【 0 0 8 0 】

ステップ 1 2 0 4 で生成情報作成処理部 9 1 2 は、ステップ 1 2 0 3 で IM 9 0 8 の貼付けが行われたコンテンツを示す情報を生成情報 9 0 9 に設定し、ステップ 1 2 0 5 では、前記設定した生成情報 9 0 9 を EXIT ゲート装置 8 1 0 へ送る。

【 0 0 8 1 】

図 1 3 は本実施形態の生成情報 9 0 9 の一例を示す図である。図 1 3 に示す様に生成情報 9 0 9 には、IM 9 0 8 の貼付けが行われたコンテンツを示す情報として、IM 9 0 8 の貼付けが行われたコンテンツデータ 9 0 7 のパス名を含むファイル名や貼付けられた IM 9 0 8 の生成日付時刻等の情報が設定されている。

【 0 0 8 2 】

図 1 4 は本実施形態のクライアント側処理の処理手順を示すフローチャートである。図 1 4 に示す様にクライアント装置 8 2 0 は、要求したコンテンツを EXIT ゲート装置 8 1 0 から受け取り、そのコンテンツの現在の内容に対応する改竄検知情報を生成して改竄を検知する処理を行う。

【 0 0 8 3 】

ステップ 1 4 0 1 でクライアント装置 8 2 0 の WWW ブラウザは、ユーザが URL (Uniform Resource Locators) を入力したかどうかを調べ、ユーザが URL を入力した場合にはその URL を受付けてステップ 1 4 0 2 へ進む。ステップ 1 4 0 2 では、ステップ 1 4 0 1 で受付けた URL のページを表示する為のリクエストを前記 URL で示される宛先へ送信する。前記 URL で示される宛先がサーバ装置 8 0 0 であり、その経路上に EXIT ゲート装置 8 1 0 がある場合には、前記リクエストは EXIT ゲート装置 8 1 0 を経由してサーバ装置 8 0 0 へ送られる。

【 0 0 8 4 】

ステップ1403では、前記送信したリクエストの結果としてHTMLデータを受信しているかどうかを調べ、HTMLデータを受信している場合にはステップ1404へ進む。

【0085】

ステップ1404では、ステップ1403で受信したHTMLデータ中にIM908が貼付けられているかどうかを調べ、IM908が貼付けられている場合にはステップ1405へ進み、IM908が貼付けられていない場合にはステップ1406へ進む。

【0086】

ステップ1405で改竄検知処理部1111は、ステップ1403で受信したHTMLデータについて、その内容に対するハッシュ値を改竄検知情報生成処理部1110により計算し、IM908中のハッシュ値と前記計算したハッシュ値とを比較して当該コンテンツの改竄が行われているかどうかを調べる。当該コンテンツの改竄が行われているかどうかを調べた結果、当該コンテンツの改竄が検知されない場合にはステップ1406へ進み、当該コンテンツの改竄を検知した場合にはステップ1407へ進む。

【0087】

ステップ1406では、ステップ1403で受信したHTMLデータに従ってページを表示する。ここで前記URLのリクエストを処理する際にEXITゲート装置810が当該ページの改竄を検知した場合には、改竄が検知されたことを示すHTMLデータがEXITゲート装置810から送られてきているので、クライアント装置820では当該ページの改竄がEXITゲート装置810で検知されたことを示す表示が行われる。

【0088】

ステップ1407では、ステップ1403で受信したHTMLデータ中にEXITゲート装置810での処理が行われたことを示す情報が含まれているかを調べ、EXITゲート装置810での処理が行われたことを示す情報が含まれている場合にはステップ1408へ進み、含まれていない場合にはステップ1409へ進む。

【 0 0 8 9 】

ステップ 1 4 0 8 では、E X I T ゲート装置 8 1 0 からクライアント装置 8 2 0 までの経路上での当該コンテンツの改竄を検知したことを示す表示を行い、ステップ 1 4 0 9 では、単に当該コンテンツの改竄を検知したことを示す表示を行う。

【 0 0 9 0 】

図 1 5 は本実施形態の E X I T ゲート側処理の処理手順を示すフローチャートである。ステップ 1 5 0 1 で E X I T ゲート装置 8 1 0 の改竄検知処理部 1 0 1 3 は、クライアント装置 8 2 0 からリクエストを受信しているかどうかを調べ、リクエストを受信している場合にはステップ 1 5 0 2 へ進む。

【 0 0 9 1 】

ステップ 1 5 0 2 では、当該リクエストで要求されているコンテンツデータ 9 0 7 をキャッシュとして保持しているかどうかを調べ、保持していない場合にはステップ 1 5 0 3 で当該リクエストをサーバ装置 8 0 0 へ送る。

【 0 0 9 2 】

ステップ 1 5 0 4 では、当該リクエストに対応する HTML データをサーバ装置 8 0 0 から受信しているかどうかを調べ、HTML データを受信している場合にはステップ 1 5 0 5 へ進む。

【 0 0 9 3 】

ステップ 1 5 0 5 で生成検査処理部 1 0 1 0 は、コンテンツの改竄を検知する為の改竄検知情報が生成されたコンテンツを示す生成情報 9 0 9 を参照する。ステップ 1 5 0 6 では、クライアント装置 8 2 0 から要求されたコンテンツについて、その改竄を検知する為の改竄検知情報が生成済みであるかどうかを調べ、改竄検知情報が生成済みである場合にはステップ 1 5 0 7 へ進む。

【 0 0 9 4 】

ステップ 1 5 0 7 で存在検査処理部 1 0 1 1 は、ステップ 1 5 0 4 で受信した HTML データ中に生成情報 9 0 9 で示された IM 9 0 8 が貼付けられているかどうかを調べ、クライアント装置 8 2 0 から要求されたコンテンツについて、そのコンテンツの改竄検知情報の有無を検査する処理を行う。生成情報 9 0 9 で示

された IM908 が貼付けられている場合にはステップ 1508 へ進み、生成情報 909 で示された IM908 が貼付けられていない場合にはステップ 1511 へ進む。

【0095】

ステップ 1508 で改竄検知処理部 1013 は、ステップ 1504 で受信した HTML データについて、その内容に対するハッシュ値を改竄検知情報生成処理部 1012 により計算し、IM908 中のハッシュ値と前記計算したハッシュ値とを比較して当該コンテンツの改竄が行われているかどうかを調べる。当該コンテンツの改竄が行われているかどうかを調べた結果、当該コンテンツの改竄が検知されない場合にはステップ 1509 へ進み、当該コンテンツの改竄を検知した場合にはステップ 1512 へ進む。

【0096】

ステップ 1509 では、ステップ 1504 で受信した HTML データであるコンテンツデータ 907 をキャッシュとして保持し、ステップ 1510 では、EXIT ゲート装置 810 での処理が行われたことを示す情報と共に当該 HTML データをクライアント装置 820 へ送信する。

【0097】

ステップ 1511 では、サーバ装置 800 上またはサーバ装置 800 から EXIT ゲート装置 810 までの経路上での当該コンテンツの改竄検知情報の除去を検知したことを示す表示を行う。またステップ 1512 では、サーバ装置 800 上またはサーバ装置 800 から EXIT ゲート装置 810 までの経路上での当該コンテンツの内容の改竄を検知したことを示す表示を行う。

【0098】

ステップ 1513 では、当該コンテンツの登録元及び更新元であるサーバ装置 800 に、サーバ装置 800 上またはサーバ装置 800 から EXIT ゲート装置 810 までの経路上で、当該コンテンツの改竄検知情報の除去または当該コンテンツの内容の改竄が行われたことを通知する処理を行う。

【0099】

またステップ 1513 では、当該コンテンツの要求元であるクライアント装置

8 2 0 に、サーバ装置 8 0 0 上またはサーバ装置 8 0 0 から E X I T ゲート装置 8 1 0 までの経路上で、当該コンテンツの改竄検知情報の除去または当該コンテンツの内容の改竄が行われたことを通知する処理を行う。

【 0 1 0 0 】

図 1 6 は本実施形態の改竄通知受信処理部 9 1 3 の処理手順を示すフローチャートである。図 1 6 に示す様にサーバ装置 8 0 0 の改竄通知受信処理部 9 1 3 は、コンテンツの改竄が行われていることを示す通知を E X I T ゲート装置 8 1 0 から受信する処理を行う。

【 0 1 0 1 】

ステップ 1 6 0 1 で改竄通知受信処理部 9 1 3 は、コンテンツの改竄が行われていることを示す通知を E X I T ゲート装置 8 1 0 から受信しているかどうかを調べ、コンテンツの改竄が行われていることを示す通知を受信している場合にはステップ 1 6 0 2 へ進む。ステップ 1 6 0 2 では、受信した通知内容を表示してサーバ装置 8 0 0 の管理者に知らせ、ステップ 1 6 0 3 では、受信した通知内容を磁気ディスク装置 9 0 3 に格納する。

【 0 1 0 2 】

以上説明した様に本実施形態のコンテンツ改竄検知装置によれば、改竄検知情報の有無を検査するので、改竄検知情報の除去による改竄の隠蔽を防止することが可能である。

【 0 1 0 3 】

また本実施形態のコンテンツ改竄検知装置によれば、クライアントとサーバの間でコンテンツの改竄を検知するので、改竄が行われた位置を特定することが可能である。

【 0 1 0 4 】

【発明の効果】

本発明によれば複数のコンテンツの構成または内容の改竄を検知するので、コンテンツの改竄を早期発見することが可能である。

【図面の簡単な説明】

【図 1】

実施形態 1 のコンテンツ改竄検知装置の概略構成を示す図である。

【図 2】

実施形態 1 の IM 生成処理部 1 1 0 の処理手順を示すフローチャートである。

【図 3】

実施形態 1 のパス名を含むファイル名に対応したハッシュ値の生成処理の概要を示す図である。

【図 4】

実施形態 1 のパス名を含むファイル名に対応したハッシュ値の生成処理の処理手順を示すフローチャートである。

【図 5】

実施形態 1 のコンテンツの内容に対応したハッシュ値の生成処理の概要を示す図である。

【図 6】

実施形態 1 のコンテンツの内容に対応したハッシュ値の生成処理の処理手順を示すフローチャートである。

【図 7】

実施形態 1 の改竄検知処理部 1 1 2 の処理手順を示すフローチャートである。

【図 8】

実施形態 2 のコンテンツ改竄検知装置の概要を示す図である。

【図 9】

実施形態 2 のサーバ装置 8 0 0 の概略構成を示す図である。

【図 1 0】

実施形態 2 の EX I T ゲート装置 8 1 0 の概略構成を示す図である。

【図 1 1】

実施形態 2 のクライアント装置 8 2 0 の概略構成を示す図である。

【図 1 2】

実施形態 2 のコンテンツ登録／更新処理の処理手順を示すフローチャートである。

【図 1 3】

実施形態 2 の生成情報 9 0 9 の一例を示す図である。

【図 1 4】

実施形態 2 のクライアント側処理の処理手順を示すフローチャートである。

【図 1 5】

実施形態 2 の E X I T ゲート側処理の処理手順を示すフローチャートである。

【図 1 6】

実施形態 2 の改竄通知受信処理部 9 1 3 の処理手順を示すフローチャートである。

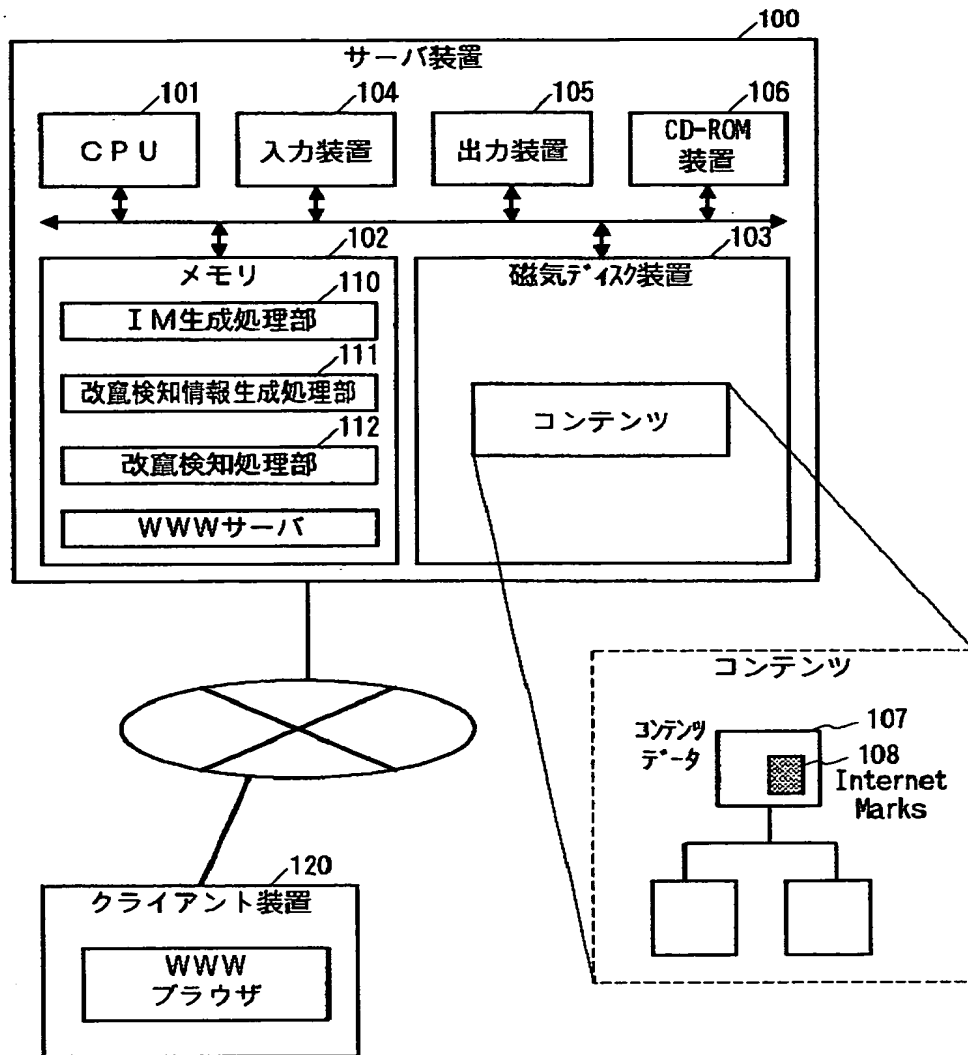
【符号の説明】

1 0 0 …サーバ装置、1 2 0 …クライアント装置、1 0 1 …CPU、1 0 2 …メモリ、1 0 3 …磁気ディスク装置、1 0 4 …入力装置、1 0 5 …出力装置、1 0 6 …CD-ROM装置、1 0 7 …コンテンツデータ、1 0 8 …IM、1 1 0 …IM生成処理部、1 1 1 …改竄検知情報生成処理部、1 1 2 …改竄検知処理部、3 0 0 及び 3 1 0 …ファイル名、3 2 0 …ハッシュ値、5 0 0 …コンテンツデータ、5 1 0 及び 5 2 0 …ハッシュ値、8 0 0 …サーバ装置、8 1 0 …E X I T ゲート装置、8 2 0 …クライアント装置、9 0 1 …CPU、9 0 2 …メモリ、9 0 3 …磁気ディスク装置、9 0 4 …入力装置、9 0 5 …出力装置、9 0 6 …CD-ROM装置、9 0 7 …コンテンツデータ、9 0 8 …IM、9 0 9 …生成情報、9 1 0 …IM生成処理部、9 1 1 …改竄検知情報生成処理部、9 1 2 …生成情報作成処理部、9 1 3 …改竄通知受信処理部、1 0 0 1 …CPU、1 0 0 2 …メモリ、1 0 0 3 …磁気ディスク装置、1 0 0 4 …入力装置、1 0 0 5 …出力装置、1 0 0 6 …CD-ROM装置、1 0 1 0 …生成検査処理部、1 0 1 1 …存在検査処理部、1 0 1 2 …改竄検知情報生成処理部、1 0 1 3 …改竄検知処理部、1 1 0 1 …CPU、1 1 0 2 …メモリ、1 1 0 3 …磁気ディスク装置、1 1 0 4 …入力装置、1 1 0 5 …出力装置、1 1 0 6 …CD-ROM装置、1 1 1 0 …改竄検知情報生成処理部、1 1 1 1 …改竄検知処理部。

【書類名】 図面

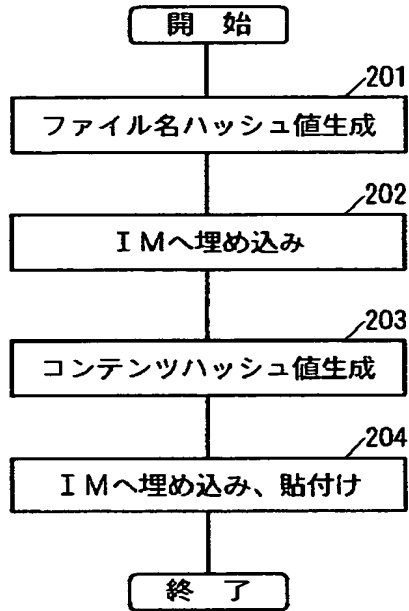
【図 1】

図 1



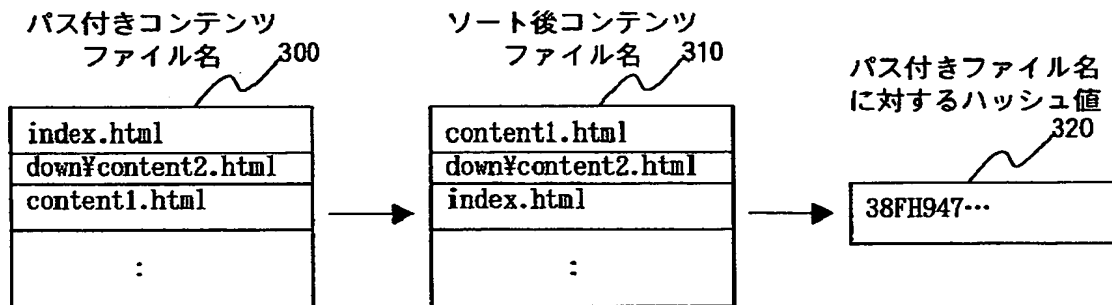
【図 2】

図 2

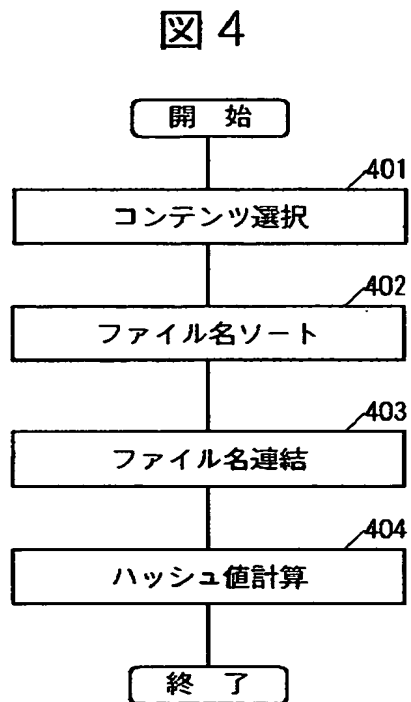


【図 3】

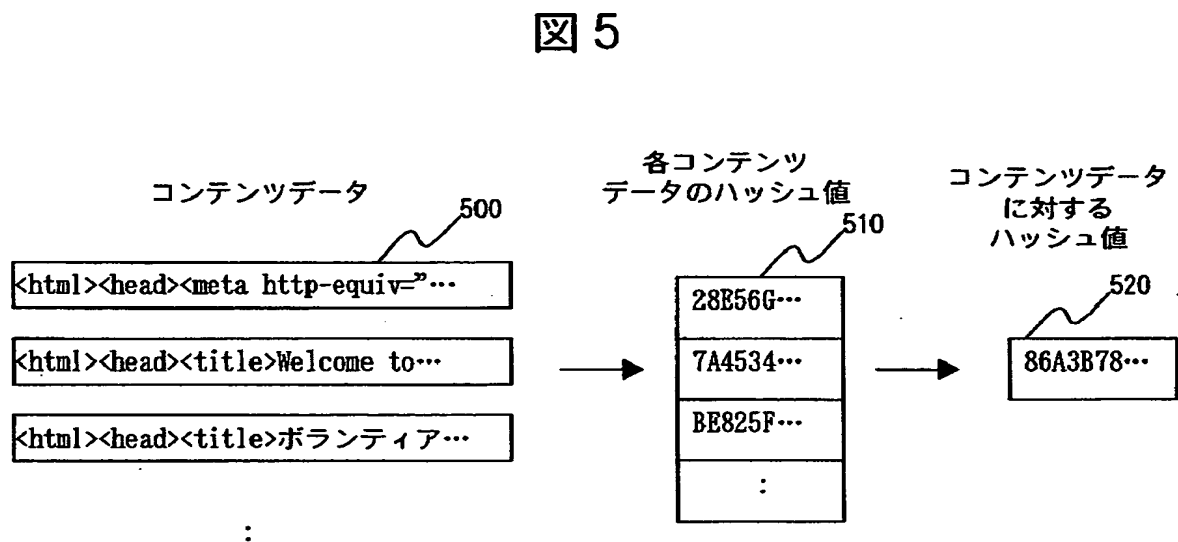
図 3



【図 4】

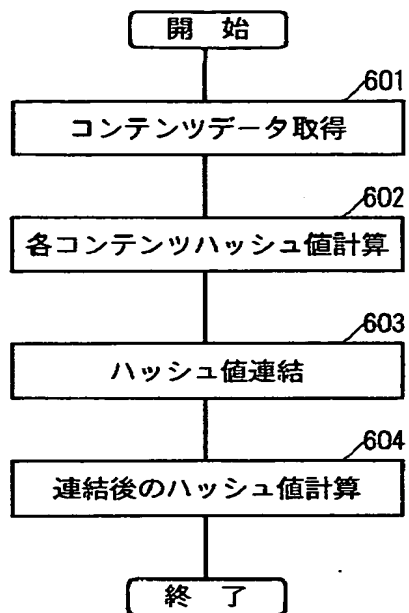


【図 5】



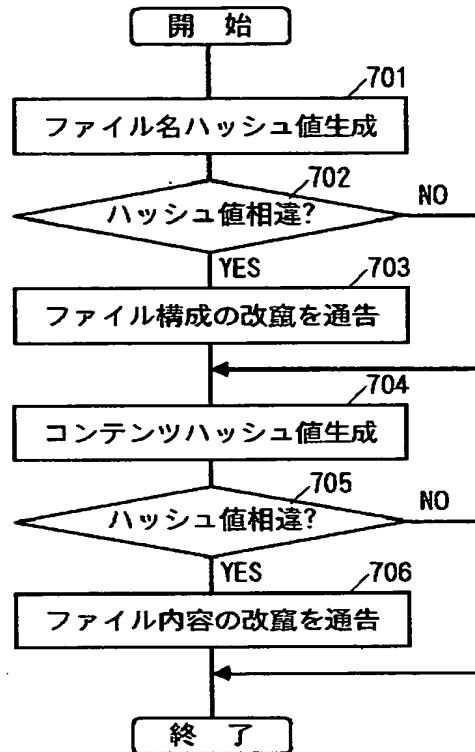
【図 6】

図 6

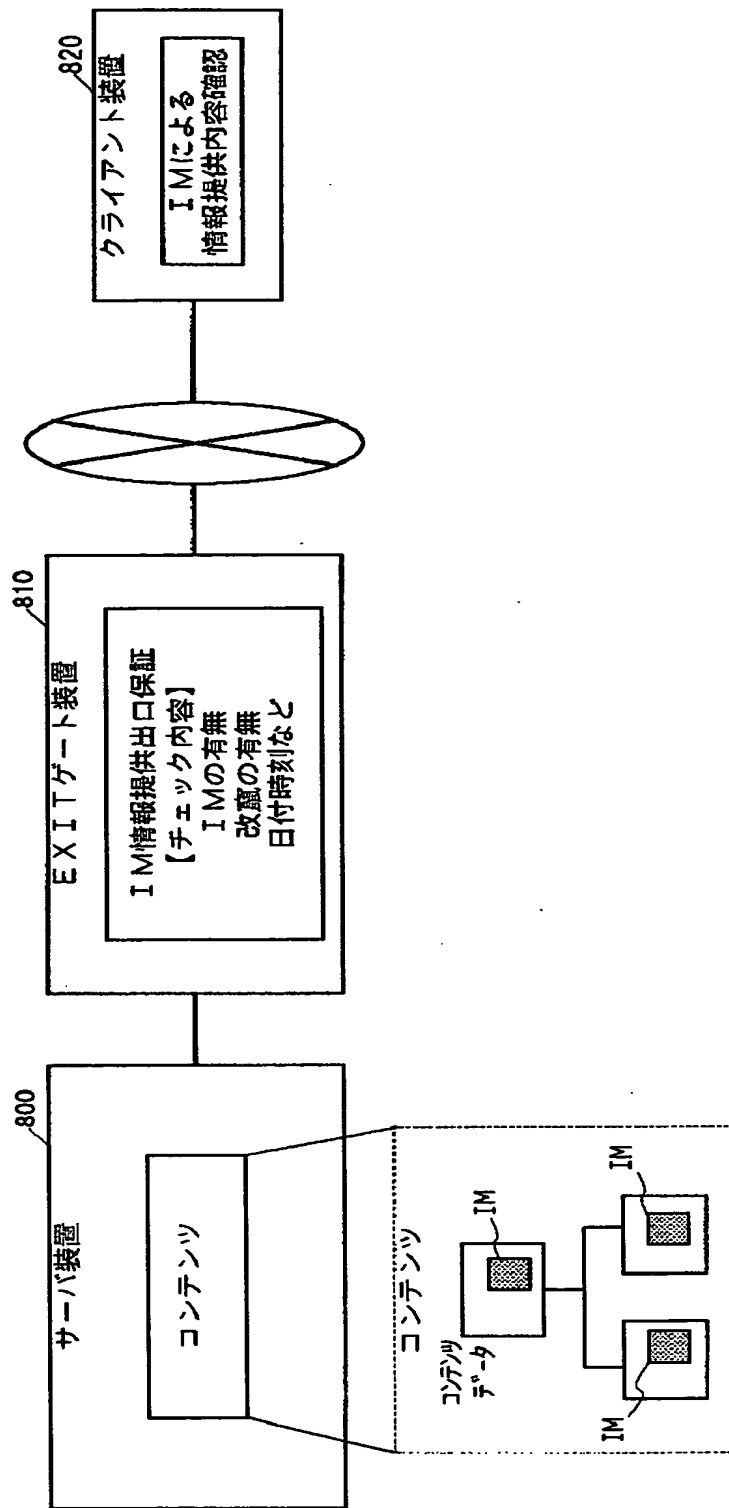


【図 7】

図 7

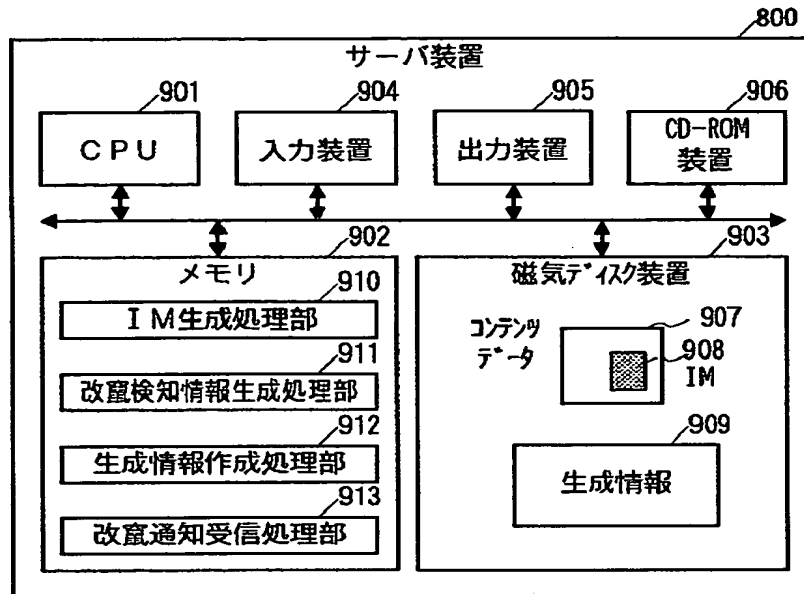


【図 8】



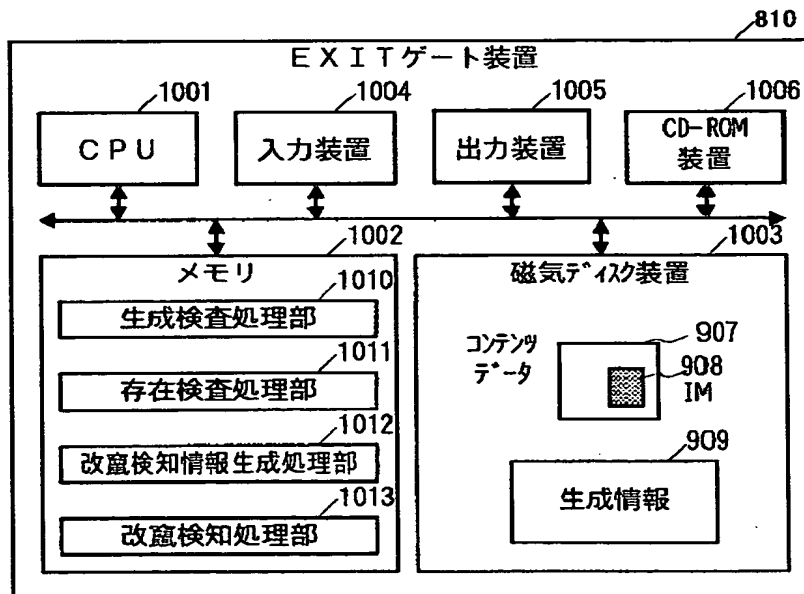
【図 9】

図 9



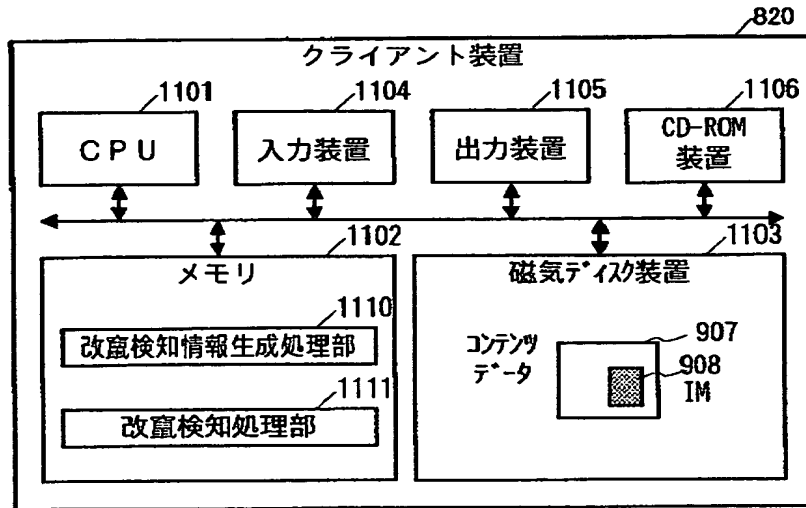
【図 1 0】

図 1 0



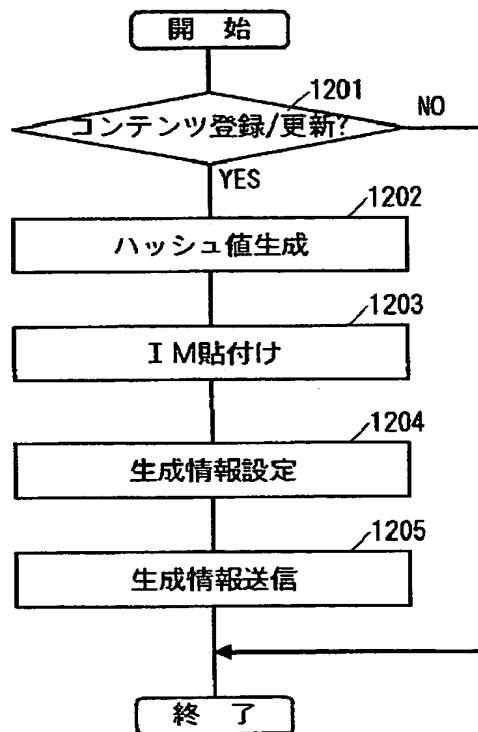
【図 1 1】

図 1 1



【図 1 2】

図 1 2



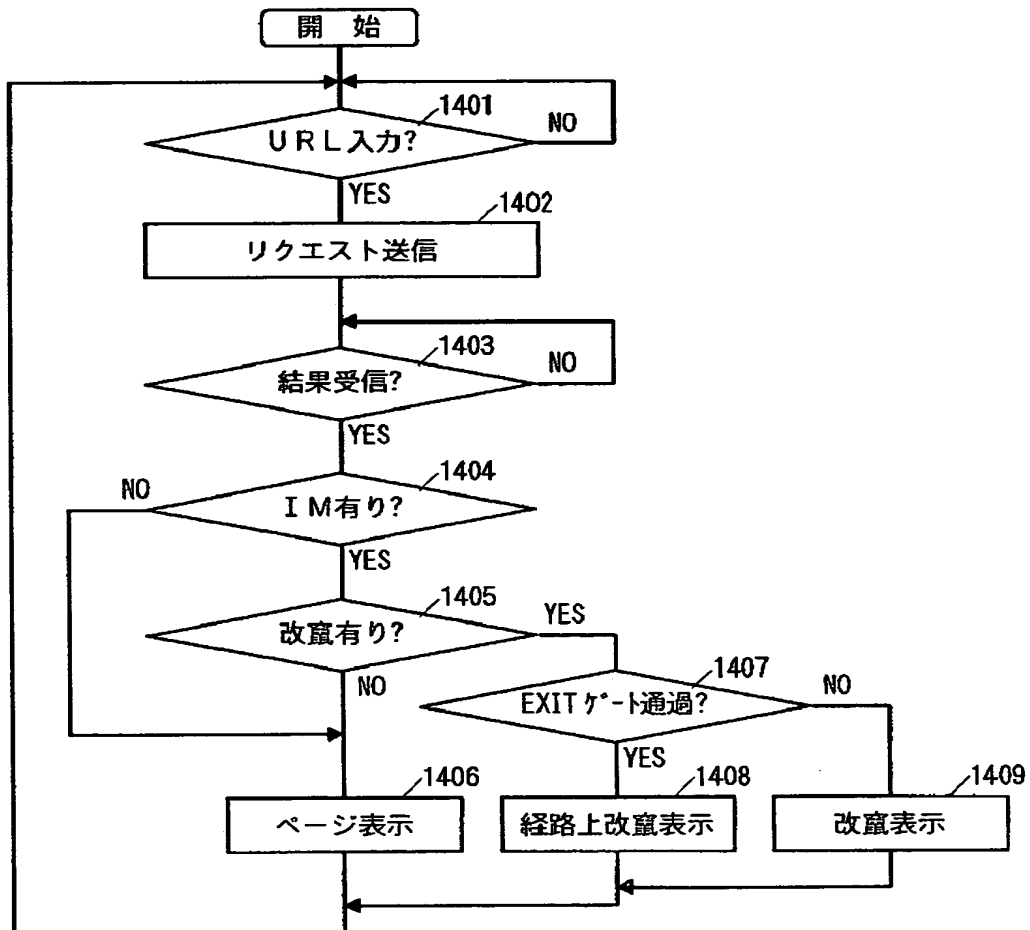
【図 1 3】

図 1 3

ファイル名	日付時刻	...
index.html	2000/3/26 11:06	...
down%content2.html	2000/3/26 11:16	...
:	:	...

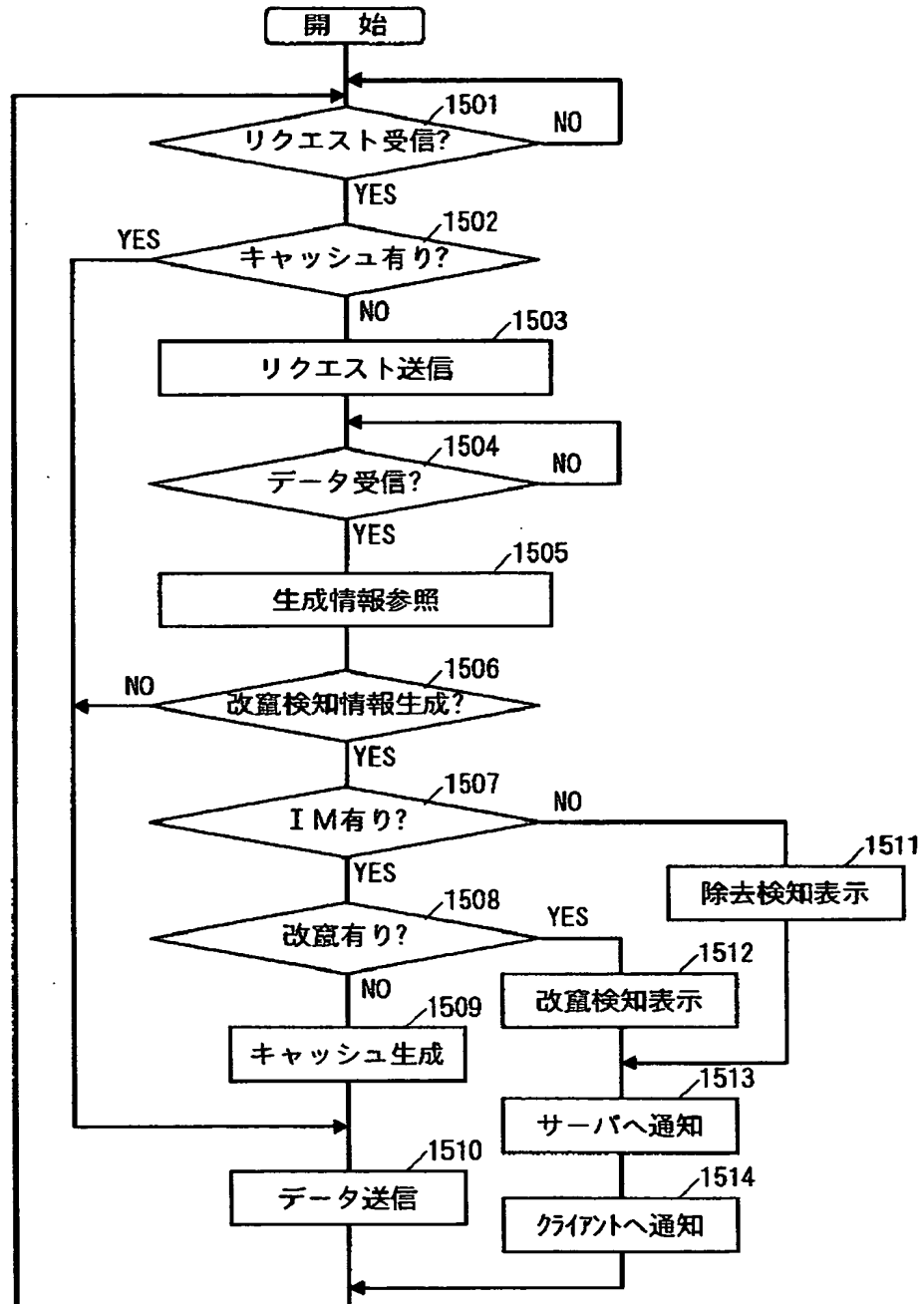
【図 1 4】

図 1 4



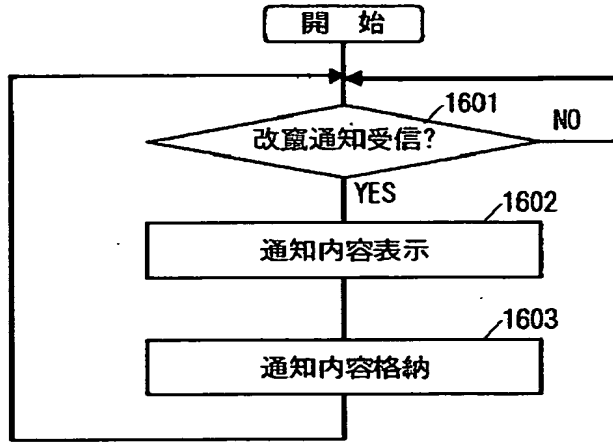
【図 1 5】

図 1 5



【図 1 6】

図 1 6



【書類名】 要約書

【要約】

【課題】 コンテンツの改竄を早期発見することが可能な技術を提供する。

【解決手段】 コンテンツの改竄を検知するコンテンツ改竄検知方法において、複数のコンテンツの現在の構成または内容に対応する改竄検知情報を生成するステップと、当該コンテンツの登録または更新時の構成または内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知するステップとを有するものである。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所